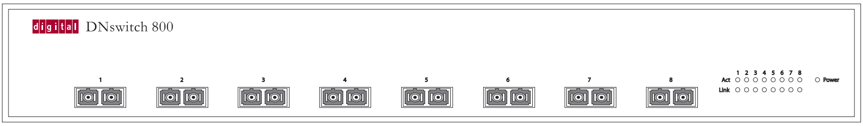
Digital Networks

digital™

DNswitch 800

Web Management Guide



DNswitch 800

Web Management Guide

Part Number: WM-DSA8G-00

March 2001

This book describes how to install, cable and use the Digital Networks DNswitch 800.

Revision/Update Information: This is a new document.

Digital Networks makes no representations that the use of its products in the manner described in this publication will not infringe on existing or future patent rights, nor do the descriptions contained in this publication imply the granting of licenses to make, use, or sell equipment or software in accordance with the description.

Possession, use, or copying of the software described in this publication is authorized only pursuant to a valid written license from Digital Networks or an authorized sublicensor.

Digital Networks
200 Brickstone Square
Andover, MA 01810

Web site: **www.dnpg.com**

FCC Class B Certification (USA)

This device complies with Part 15 of the FCC Rules. Operation is subject to the following conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Warning! This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the distance between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from the one which the receiver is connected to.
- Consult the dealer or an experienced radio/TV technician for help.

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Attach 62.5/125 or 50/125 µm multimode fiber cable to the SC ports.

Note: In order to maintain compliance with the limits of a Class B digital device, Digital Networks requires that you use a quality interface cable when connecting to this device. Changes or modifications not expressly approved by Digital Network could void the user's authority to operate this equipment. Suggested cable type is 62.5/125 or 50/125 µm multimode fiber cable for SC port connections.

Canada Department of Communications - Class B

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of the Department of Communications.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques," NMB-003 édictée par le ministère des Communications.

BSMI Class A (Taiwan)

警告使用者：這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

VCCI Class B Compliance (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると受信障害を引き起こすことがあります。

取り扱い説明書に従って正しい取り扱いをして下さい。

CE Mark Declaration of Conformance for EMI and Safety

This is to certify that this product complies with ISO/IEC Guide 22 and EN45014.

It conforms to the following specifications:

EMC:	EN55022(1988)/CISPR-22(1985)	class B
	EN60555-2(1995)	class B
	EN60555-3	
	IEC1000-4-2(1995)	4kV CD, 8kV AD
	IEC1000-4-3(1995)	3V/m
	IEC1000-4-4(1995)	1kV - (power line), 0.5kV - (signal line)
	IEC1000-4-6(1995)	3Vrms

This product complies with the requirements of the Low Voltage Directive 73/23/EEC and the EMC Directive 89/336/EEC.

Safety Compliance

Warning: Fiber Optic Port Safety

CLASS I
LASER DEVICE

When using a fiber optic port, never look at the transmit laser while it is powered on. Also, never look directly at the fiber TX port and fiber cable ends when they are powered on.

Avertissment: Ports pour fibres optiques - sécurité sur le plan optique

DISPOSITIF LASER
DE CLASSE I

Ne regardez jamais le laser tant qu'il est sous tension. Ne regardez jamais directement le port TX (Transmission) à fibres optiques et les embouts de câbles à fibres optiques tant qu'ils sont sous tension.

Warnhinweis: Faseroptikanschlüsse - Optische Sicherheit

LASERGERÄT
DER KLASSE I

Niemals ein Übertragungslaser betrachten, während dieses eingeschaltet ist. Niemals direkt auf den Faser-TX-Anschluß und auf die Faserkabelenden schauen, während diese eingeschaltet sind.

Underwriters Laboratories Compliance Statement

Important! Before making connections, make sure you have the correct cord set. Check it (read the label on the cable) against the following:

Operating Voltage	**Cord Set Specifications**
120 Volts	UL Listed/CSA Certified Cord Set
	Minimum 18 AWG
	Type SVT or SJT three conductor cord
	Maximum length of 15 feet
	Parallel blade, grounding type attachment plug rated 15A, 125V
240 Volts (Europe only)	Cord Set with H05VV-F cord having three conductors with minimum diameter of 0.75 mm^2
	IEC-320 receptacle
	Male plug rated 10A, 250V

The unit automatically matches the connected input voltage. Therefore, no additional adjustments are necessary when connecting it to any input voltage within the range marked on the rear panel.

Wichtige Sicherheitshinweise (Germany)

1. Bitte lesen Sie diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den späteren Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwenden Sie keine Flüssigoder Aerosolreiniger. Am besten eignet sich ein angefeuchtetes Tuch zur Reinigung.
4. Die Netzanschlu ßsteckdose soll nahe dem Gerät angebracht und leicht zugänglich sein.
5. Das Gerät ist vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sicheren Stand zu achten. Ein Kippen oder Fallen könnte Beschädigungen hervorrufen.
7. Die Belüftungsöffnungen dienen der Luftzirkulation, die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollte auch nichts auf der Leitung abgestellt werden.
10. Alle Hinweise und Warnungen, die sich am Gerät befinden, sind zu beachten.
11. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
12. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. elektrischen Schlag auslösen.
13. Öffnen sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
14. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
    a. Netzkabel oder Netzstecker sind beschädigt.
    b. Flüssigkeit ist in das Gerät eingedrungen.

c. Das Gerät war Feuchtigkeit ausgesetzt.
d. Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.

15. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden. Für einen Nennstrom bis 6A und einem Gerätegewicht größer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm^2 einzusetzen.

Der arbeitsplatzbezogene Schalldruckpegel nach DIN 45 635 Teil 1000 beträgt 70dB(A) oder weniger.

Table of Contents

1. OVERVIEW

Digital Networks WebView Description

This user guide describes Digital Networks WebView, a Web browser-based utility which allows you to remotely configure and manage Digital Networks products, including the DNswitch 800. There is no software to install as Web management capability is built into the switch’s management.

Digital Networks WebView provides a graphical, real-time representation of the front panel on the DNswitch 800. This graphic, along with additionally defined areas of the browser interface, allow you to interactively configure the switch, monitor its status, and view statistical information.

Digital Networks WebView provides a simple, intuitive method for managing the DNswitch 800. This switch can also be managed via the serial console, Telnet, or SNMP.

Features

- Switch configuration and monitoring from any Java-enabled browser (Preferred browsers include Internet Explorer 4.0 or above, or Netscape Navigator 4.0 or above)
- Easy to navigate menuing system
- Detailed parameter descriptions using the Help button
- Switch operating status viewing front panel color indications
- Alarm configuration capability
- Web management enable

System Requirements

The requirements for running Digital Networks WebView are relatively simple. You will need a Java-enabled, frames-capable Web browser and a TCP/IP network connection to the switch, whether over a local network, a remote private network, or over the Internet.

When connecting over the Internet, the integrity of your connection will have an impact on the speed and performance of tasks. If your connection is subject to prohibitive periods of network congestion, or experiences high packet loss, you may need to consider a different Internet service provider.

In addition, Digital Networks WebView uses SNMP for some of its communications with the switch. This may cause problems when the application is run across some Internet firewalls, which may be configured to disallow SNMP access.

Conventions

This guide uses the following user input conventions:

- When you read “Select,” use the mouse to either select the link identified by a hand icon, or select the identified button or area.
- When you read “Enter,” type in the text and select the button identified in the procedure.

2. USING WEB-BASED MANAGEMENT

Setting Up Web Management

Before running Web-based management, some basic configuration of the switch may need to be performed. The following information at a minimum must be configured or known for the switch to be managed:

- IP Address
- Administrator password
- HTTP Server Enable

In addition, several other parameters may need to be configured or known to properly communicate with the switch or allow full management capability. These include:

- Default Gateway
- Trap Destination and Community Name

Configuration of these items may be made from the console user interface, which is accessible via either the serial console or Telnet. Refer to the DNswitch 800 User's Guide that came with your system for more information about setting up either of these connections to the switch. The following subsections describe the required configuration.

Setting an IP Address

The IP address for the switch must be set before it can be managed with Digital Networks WebView. The switch IP address may be automatically set using the BootP protocol, in which case the actual address assigned to the switch must be known. Refer to the DNswitch 800 Management Guide.

The IP address may alternatively be set manually as follows:

1. Starting at the Main Menu of the console user interface, select Management Setup Menu / Network Configuration / IP Configuration.
2. Select IP Address from the menu and enter the IP address.
3. Select Subnet Mask from the menu and enter the appropriate mask.
4. Press <APPLY>.

Setting a Default Gateway

The default gateway parameter defines the IP address of a router or other network device to which IP packets are to be sent if destined for a subnet outside of that in which the switch is operating. This parameter must be set if you are attempting to manage the switch using Digital Networks WebView from a remote network or across the Internet.

1. Starting at the Main Menu of the console user interface, select Management Setup Menu / Network Configuration / IP Configuration.

2. Select Gateway IP from the menu and enter the router IP address. Press <APPLY>.

Setting the Administrator Password

Management access to the switch using Digital Networks WebView is restricted based on the an administrator password. Administrators have read/write access for parameters governing the switch. You should therefore assign a password to the default administrator (User Name: admin) as soon as possible, and store it in a safe place. (If for some reason your password is lost, or you cannot gain access to the system's configuration program, contact Digital Networks Technical Support for assistance.)

1. Starting at the Main Menu of the console user interface, select Management Setup Menu / Console Login Configuration.

2. Move to the Password field for the User Name "admin" in this menu, and enter the password. Press <APPLY>.

Setting Trap Destinations

If you wish to record SNMP traps, or events, generated by the switch, you must configure the destination for IP Trap Managers. A trap destination is the IP address of the system being used to manage the device, in this case the IP address of the computer system on which Digital Networks WebView is being run.

1. Starting at the Main Menu of the console user interface, select Management Setup Menu / SNMP Configuration / IP Trap Managers.

2. Select an entry for an IP Trap Manager from the menu, then enter the IP address and community name.

3. Move to the Status field, and use the Space bar to select ENABLED.

4. Press <APPLY>.

Enabling Web Management

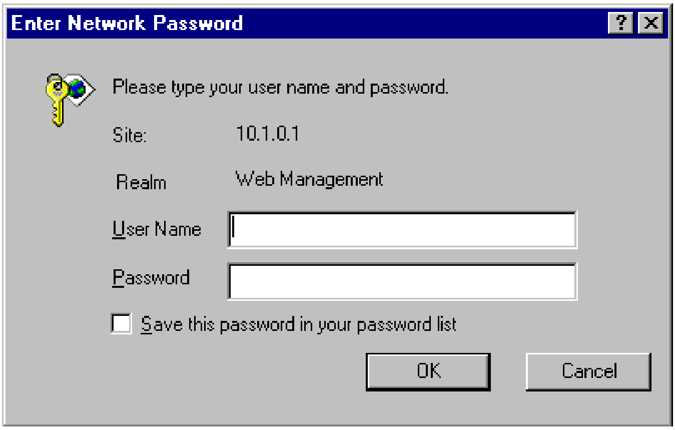
The HTTP Configuration menu is used to enable or disable the ability to manage the switch with Web management. The HTTP Server parameter must be set to ENABLED before Digital Networks WebView can be used to manage the switch. If it is desired to disallow Web management of the switch, this parameter should be set to DISABLED

1. Starting at the Main Menu of the console user interface, select Management Setup Menu / Network Configuration / HTTP Configuration.
2. Select HTTP Server, and use the Space bar to toggle between ENABLED and DISABLED.

Starting and Stopping Digital Networks WebView

Do the following to use Digital Networks WebView:

1. Start a Java-enabled Web browser from any machine with network access to the switch. (Preferred browsers include Internet Explorer 4.0 or above, or Netscape Navigator 4.0 or above.)
2. Enter the IP address for the switch you want to manage in the URL field of the browser.
3. The screen shown below will appear, prompting you to enter the user name and password for management access.



Please type your user name and password.

Site: 10.1.0.1

Realm Web Management

Use the name for the default administrator (admin), and the password previously entered in the Setting Up Web Management section. This will allow read/write access to the switch.

The full application will now launch. A four-frame page will display with the product graphic located in the upper right hand frame.

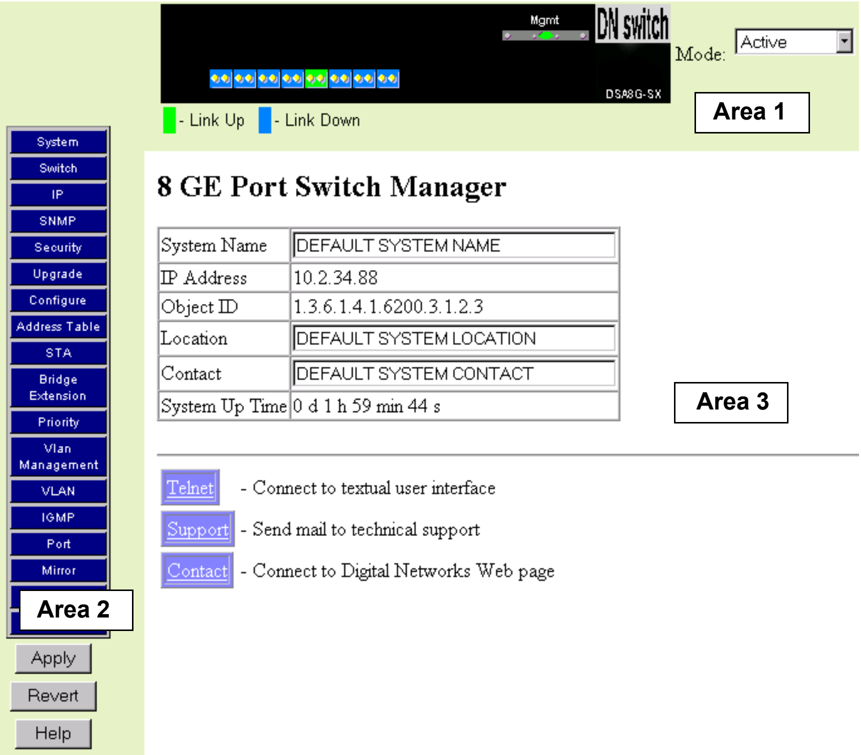
4. To stop Digital Networks WebView, close the Web browser application.

Digital Networks WebView User Interface

The Digital Networks WebView user interface provides access to various switch configuration and management screens, allows you to view performance statistics, and permits you to graphically monitor system status.

Areas of the User Interface

Figure 2-1 shows the Digital Networks WebView user interface. The user interface is divided into four distinct areas as described in Table 2-1.



Mode: Active

🟩 - Link Up 🟦 - Link Down

8 GE Port Switch Manager

System Name	DEFAULT SYSTEM NAME
IP Address	10.2.34.88
Object ID	1.3.6.1.4.1.6200.3.1.2.3
Location	DEFAULT SYSTEM LOCATION
Contact	DEFAULT SYSTEM CONTACT
System Up Time	0 d 1 h 59 min 44 s

Telnet - Connect to textual user interface

Support - Send mail to technical support

Contact - Connect to Digital Networks Web page

Figure 2-1. Digital Networks WebView User Interface

Table 2-1. Areas of the User Interface

Area	Function
1	Presents a graphical near real-time image of the front panel of the selected switch. This area displays the switch’s ports, showing port activity, duplex mode, or flow control, depending on the specified mode. Various areas of the graphic can be selected for performing management functions, including the ports, management, or the case.
2	Displays a list of links allowing you to go to the associated menu or screen by selecting the item.
3	Presents system information based on your selection.

Table 2-2 describes configuration and system information functions available In Area 2.

Table 2-2. Area 2 Functions

Function	Description
System	Provides basic system description, including contact information.
Switch	Shows hardware/firmware version numbers and power status of the switch.
IP	Includes boot state, IP address, and Telnet session count.
SNMP	Configures communities and trap managers; and activates traps.
Security	Sets password for system access.
Upgrade	Downloads new version of firmware to update your system.
Configure	Allows you to save/restore the switch configuration to a file on a server.
Address Table	Provides full listing or unicast addresses, sorted by address or VLAN.
STA	Enables Spanning Tree Algorithm; also sets parameters for switch priority, hello time, maximum message age, and forward delay; as well as port priority and path cost.
Bridge Extension	Displays/configures extended bridge capabilities provided by this switch, including support for traffic classes, GMRP multicast filtering, and VLAN extensions.
Priority	Configures default port priorities and queue assignments.
VLAN Management	Allows you to restrict management access to the switch to one VLAN.
VLAN	Configures VLAN group members, automatic registration with GVRP, and other port-specific VLAN settings.
IGMP	Configures IGMP multicast filtering.
Port	Enables any port, sets communication mode to auto-negotiation, full duplex or half duplex, and enables/disables flow control.
Mirror	Sets the source and target ports for mirroring.
Trunk	Specifies ports to group into aggregate trunks.
Statistics	Displays statistics on network traffic passing through the selected port.

Configuration Options

Web pages that include selection options have a drop-down list with a “Select” button to confirm the selection. Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the “Apply” button at the bottom of the page to confirm the new setting. The following table summarizes the Web page configuration buttons.

Table 2-3. Web Page Configuration Buttons

Button	Action
Select	Sets the selected option from the drop-down list.
Apply	Sets specified values in the SNMP agent.
Revert	Cancels specified values prior to pressing the “Apply” button.
Refresh	Immediately updates values from the SNMP agent.
Help	Provides help on using the Web management interface.

Using Help

General Digital Networks WebView help guidelines are available by using the Help button in Area 3.

3. CONFIGURING AND MONITORING THE SWITCH

This section, arranged by topic, describes how to perform common monitoring and configuration tasks on a DNswitch 800 using Digital Networks WebView. After you have properly configured the switch, and started Digital Networks WebView, you can perform any of the tasks described in the following sections.

Screen Hierarchy

The contents of this chapter are arranged following the structure shown in Figure 3-1.

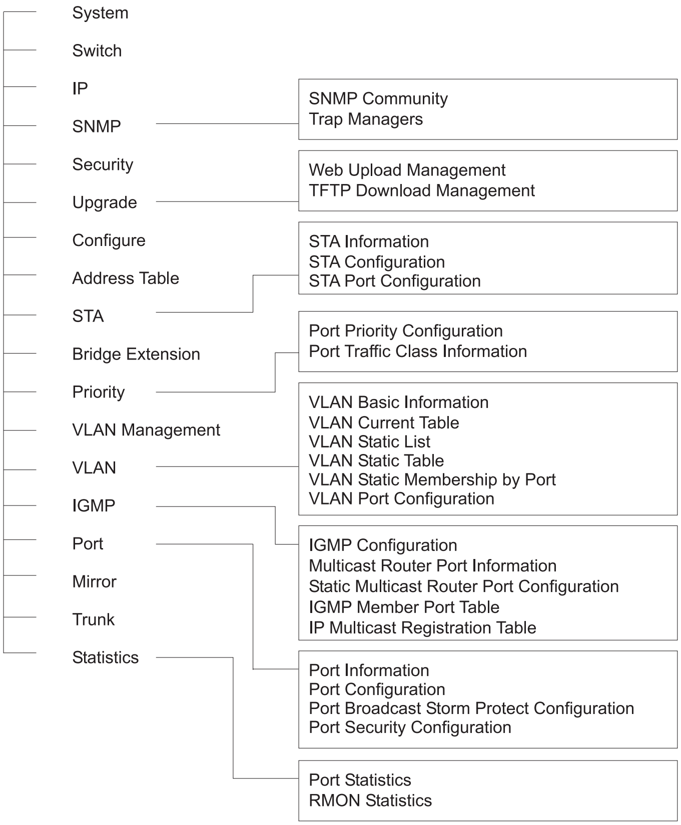
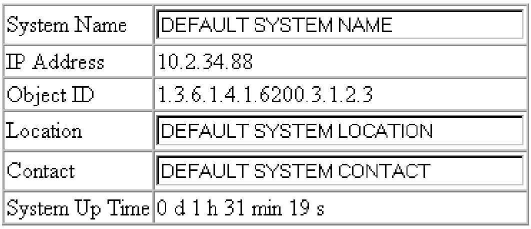


Figure 3-1. Digital Networks WebView Screen Hierarchy

System Information

Use the System Information screen to display descriptive information about the switch, or for quick system identification as shown in the following figure and table.



System Name	DEFAULT SYSTEM NAME
IP Address	10.2.34.88
Object ID	1.3.6.1.4.1.6200.3.1.2.3
Location	DEFAULT SYSTEM LOCATION
Contact	DEFAULT SYSTEM CONTACT
System Up Time	0 d 1 h 31 min 19 s

Figure 3-2. System Information

Parameter	Description
System Name[1]	Name assigned to the switch system.
Object ID	MIB II object identifier for switch's network management subsystem.
IP Address[2]	IP address of the switch you are managing. The switch's management supports SNMP over UDP/IP transport protocol. In this environment, all systems on the Internet, such as network interconnection devices and any PC accessing the switch (or running management software) must have an IP address. Valid IP addresses consist of four decimal numbers, of 0 to 255, separated by periods. Anything outside of this format will not be accepted by the configuration program.
Location[1]	Specifies the area or location where the system resides.
Contact[1]	Contact person for the system.
System Up Time	Length of time the current management software has been running.

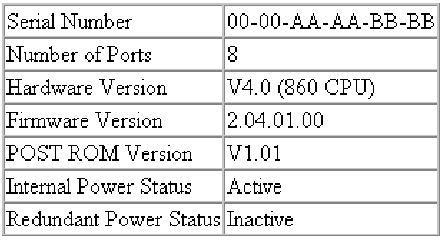
[1] Maximum string length is 255, but the screen only displays 45 characters. You can use the arrow keys to browse the whole string.

[2] The default value is 10.1.0.1

Switch Information

Use the Switch Information screen to display hardware/firmware version numbers for the switch, as well as the power status of the system.

Main Board



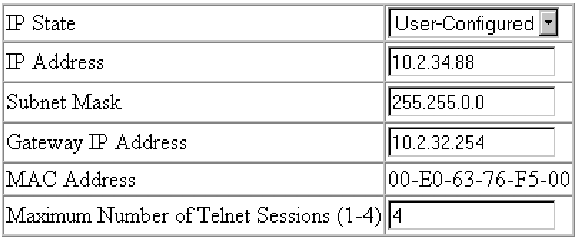
Serial Number	00-00-AA-AA-BB-BB
Number of Ports	8
Hardware Version	V4.0 (860 CPU)
Firmware Version	2.04.01.00
POST ROM Version	V1.01
Internal Power Status	Active
Redundant Power Status	Inactive

Figure 3-3. Switch Information - Main Board

Parameter	Description
Serial Number	Serial number of the main board.
Number of Ports	Number of ports on the switch.
Hardware Version	Hardware version of the main board.
Firmware Version	System firmware version in ROM.
POST ROM Version	Management's Power-on Self-test version.
Internal Power Status	Power status for the switch.
Redundant Power Status	Redundant power status for the switch.

IP Configuration

Use the IP Configuration screen to set the bootup option, configure the Ethernet IP address for the switch, or set the number or concurrent Telnet sessions allowed. The screen shown below is described in the following table.



IP State	User-Configured
IP Address	10.2.34.88
Subnet Mask	255.255.0.0
Gateway IP Address	10.2.32.254
MAC Address	00-E0-63-76-F5-00
Maximum Number of Telnet Sessions (1-4)	4

Figure 3-4. IP Configuration

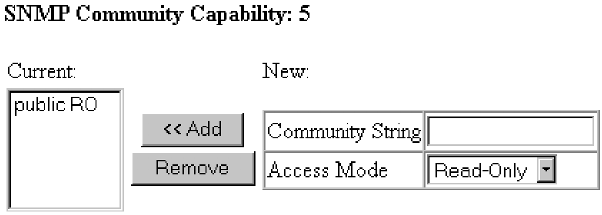
Parameter	Default	Description
IP State	BootP-Get-IP	Specifies whether IP functionality is enabled via manual configuration, or set by Boot Protocol (BootP). Options include: BootP Get IP - IP is enabled but will not function until a BootP reply has been received. BootP requests will be periodically broadcast by the switch in an effort to learn its IP address. (BootP values include the IP address, default gateway, and subnet mask.) User-Configured - IP functionality is enabled based on the default or user specified IP Configuration.
IP Address	10.1.0.1	IP address of the switch you are managing. The switch supports SNMP over UDP/IP transport protocol. In this environment, all systems on the Internet, such as network interconnection devices and any PC accessing the switch (or running management software) are assigned an IP address. Valid IP addresses consist of four numbers, of 0 to 255, separated by periods. Anything outside of this format will not be accepted by the configuration program.
Subnet Mask	255.255.0.0	Subnet mask of the switch. This mask identifies the host address bits used for routing to specific subnets.
Gateway IP		Gateway used to pass trap messages from the switch to the management station. Note that the gateway must be defined if the management station is located in a different IP segment.
MAC Address		Physical address of the switch.
Number of Telnet sessions	4	Sets the number of concurrent Telnet sessions allowed to access the switch.

SNMP Configuration

Use the SNMP Configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP). The switch includes an SNMP agent which monitors the status of its hardware, as well as the traffic passing through its ports. A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the switch are controlled by community strings. To communicate with the switch, the NMS must first submit a valid community string for authentication. The options for configuring community strings and related trap functions are described in the following figures and table.

SNMP Community

The following figure and table describe how to configure the community strings authorized for management access. Up to 5 community names may be entered.



SNMP Community Capability: 5

Current:

public RO

New:

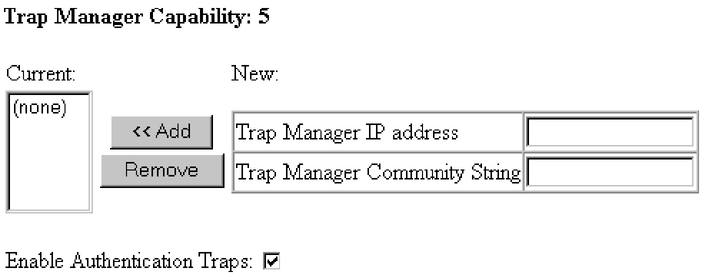
Community String	
Access Mode	Read-Only

Figure 3-5. SNMP Community

Parameter	**Description**
SNMP Community Capability	Up to 5 community strings may be used.
Add/Remove	Add/remove strings from the active list.
Community String	A community entry authorized for management access. (The maximum string length is 19 characters).
Access Mode	Management access is restricted to Read Only or Read/Write.

Trap Managers

The following figure and table describe how to specify management stations that will receive authentication failure messages or other trap messages from the switch. Up to 5 trap managers may be entered.



Trap Manager Capability: 5

Current: (none)

New:

Trap Manager IP address

Trap Manager Community String

Enable Authentication Traps: ☑

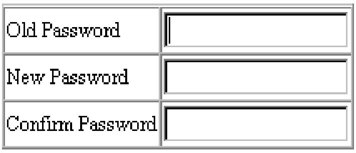
Figure 3-6. Trap Managers

Parameter	**Description**
Trap Manager Capability	Up to 5 trap managers may be used.
Trap Manager IP Address	IP address of the trap manager.
Trap Manager Community String	A community authorized to receive trap messages.
Add/Remove	Add/remove strings from the active list.
Enable Authentication Traps	Issues a trap message to specified IP trap managers whenever authentication of an SNMP request fails. Default: enabled

Security Configuration

Use the Security Configuration screen to restrict management access based on a specified password. The Administrator has write access for parameters governing the switch. You should therefore assign a password to the Administrator as soon as possible, and store it in a safe place. (If for some reason your password is lost, or you cannot gain access to the system's configuration program, contact Digital Networks Technical Support for assistance.)

Change Password



Old Password	
New Password	
Confirm Password	

Figure 3-7. Change Password

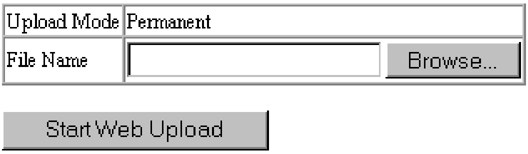
This password is for the system Administrator, with access privilege of Read/Write for all screens. Passwords can consist of up to 11 alphanumeric characters and are not case sensitive.
(User name: admin; default password: null)

Firmware Upgrade Options

You can upgrade system firmware via a Web browser, a TFTP server, or a direct connection to the console port (refer to the DNswitch 800 Management Guide).

Web Upload Management

Use the Web Upload Management menu to load software updates into the switch. The upload file should be a DNswitch 800 binary file from Digital Networks; otherwise the switch will not accept it. The success of the upload operation depends on the quality of the network connection. After uploading the new software, the switch will automatically restart itself. Parameters shown on this screen are indicated in the following figure and table.



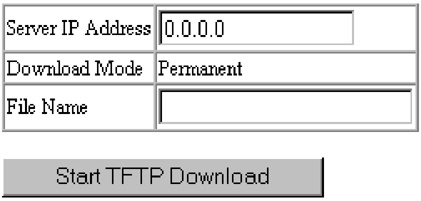
Upload Mode	Permanent
File Name	

Figure 3-8. Web Upload Management

Parameter	Description
Upload Mode	Indicates an upload to permanent flash ROM.
File Name	The binary file to download. Use the browse button to locate the file on your local network.
Start Web Upload	Starts uploading the file over the network.

TFTP Download Management

Use the TFTP Download Management menu to load software updates into the switch. The download file should be a DNswitch 800 binary file from Digital Networks; otherwise the switch will not accept it. The success of the download operation depends on the accessibility of the TFTP server and the quality of the network connection. After downloading the new software, the switch will automatically restart itself. Parameters shown on this screen are indicated in the following figure and table.



Server IP Address	0.0.0.0
Download Mode	Permanent
File Name	

Figure 3-9. TFTP Download Management

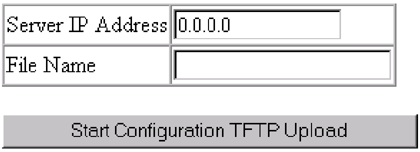
Parameter	Description
Server IP Address	IP address of a TFTP server.
Download Mode	Indicates a download to permanent flash ROM.
File Name	The binary file to download.
Start TFTP Download	Issues request to TFTP server to download the specified file.

Configuration Save and Restore

Use the Configure screen to save the switch configuration settings to a file on a TFTP server. The file can be later downloaded to the switch to restore the switch's settings. The success of the operation depends on the accessibility of the TFTP server and the quality of the network connection.

Configuration Upload Management

Use the Configuration Upload Management to save the switch configuration to a file on a TFTP sever. Parameters shown on this screen are indicated in the following figure and table.



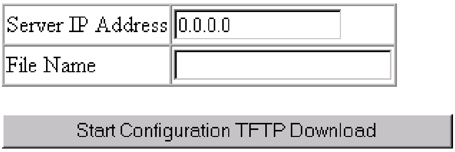
Server IP Address	0.0.0.0
File Name	

Figure 3-10. Configuration Upload Management

Parameter	Description
Server IP Address	IP address of a TFTP server.
File Name	The name of the file to contain the switch configuration settings.
Start Configuration TFTP Upload	Issues a request to upload the configuration settings to the specified file on the TFTP server.

Configuration Download Management

Use the Configuration Download Management to restore switch configuration settings from a file on a TFTP sever. Parameters shown on this screen are indicated in the following figure and table.



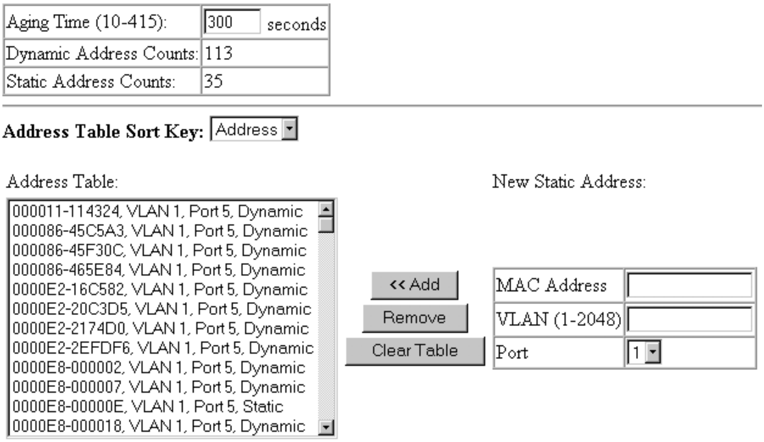
Server IP Address	0.0.0.0
File Name	

Figure 3-11. Configuration Download Management

Parameter	Description
Server IP Address	IP address of the TFTP server.
File Name	The name of the file that contains the switch configuration settings you wish to restore.
Start Configuration TFTP Download	Issues a request to the TFTP server to download the specified file.

Address Table Configuration

The Address Table contains the unicast MAC addresses and VLAN identifier associated with each port (that is, the source port associated with the address and VLAN), sorted by MAC address or VLAN. You can also clear the entire address table, or information associated with a specific address; or set the aging time for deleting inactive entries. The information displayed in the Address Table is indicated in the following figure and table.



Aging Time (10-415):	300 seconds
Dynamic Address Counts:	113
Static Address Counts:	35

Address Table Sort Key: Address

Address Table:

```
000011-114324, VLAN 1, Port 5, Dynamic
000086-45C5A3, VLAN 1, Port 5, Dynamic
000086-45F30C, VLAN 1, Port 5, Dynamic
000086-465E84, VLAN 1, Port 5, Dynamic
0000E2-16C582, VLAN 1, Port 5, Dynamic
0000E2-20C3D5, VLAN 1, Port 5, Dynamic
0000E2-2174D0, VLAN 1, Port 5, Dynamic
0000E2-2EFDF6, VLAN 1, Port 5, Dynamic
0000E8-000002, VLAN 1, Port 5, Dynamic
0000E8-000007, VLAN 1, Port 5, Dynamic
0000E8-00000E, VLAN 1, Port 5, Static
0000E8-000018, VLAN 1, Port 5, Dynamic
```

New Static Address:

MAC Address	
VLAN (1-2048)	
Port	1

Figure 3-12. Address Table

Parameter	Description
Aging Time	Time-out period in seconds for aging out dynamically learned forwarding information. Range: 10 - 415 secs; default: 300 secs.
Dynamic Address Counts	The number of dynamically learned addresses currently in the table.
Static Address Counts	The number of static addresses currently in the table.
Address Table	All entries, sorted by address or VLAN ID.
Address Table Sort Key	The system displays the MAC address of each node and port whose address table includes this MAC address, the associated VLAN(s), and the address status (i.e., dynamic or static).
New Static Address	Use these fields to add or remove a static entry to the address table. Indicate the address, port and VLAN group when adding a new entry.
Add/Remove	Adds/removes selected address.
Clear Table	Removes all addresses from the address table.

STA (Spanning Tree Algorithm)

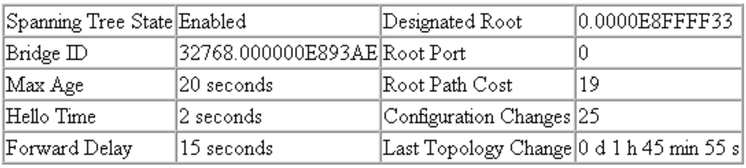
The Spanning Tree Algorithm can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network. For a more detailed description of how to use this algorithm, refer to Appendix A, “Spanning Tree Concepts,” in the Management Guide.

Spanning Tree Information

The Spanning Tree Information screen displays a summary of the STA information for the overall bridge or for a specific port. To make any changes to the parameters for the Spanning Tree, use the STA Configuration and STA Port Configuration screens.

Spanning Tree

The parameters shown in the following figure and table describe the current bridge STA Information.



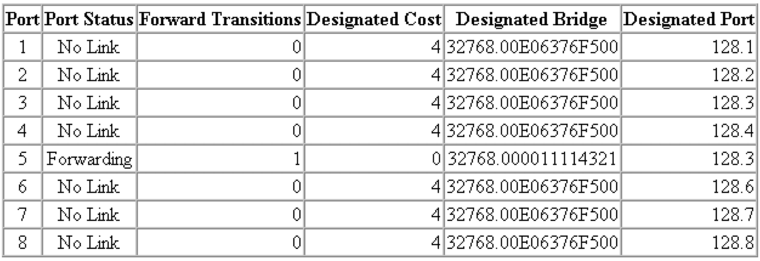
Spanning Tree State	Enabled	Designated Root	0.0000E8FFFF33
Bridge ID	32768.000000E893AE	Root Port	0
Max Age	20 seconds	Root Path Cost	19
Hello Time	2 seconds	Configuration Changes	25
Forward Delay	15 seconds	Last Topology Change	0 d 1 h 45 min 55 s

Figure 3-13. STA Information - Spanning Tree

Parameter	Description
Spanning Tree State	Shows if the switch is enabled to participate in an STA-compliant network.
Bridge ID	A unique identifier for this bridge, consisting of bridge priority plus MAC address (where the address is normally taken from Port 1).
Max Age	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure.
Hello Time	The time interval (in seconds) at which the root device transmits a configuration message.
Forward Delay	The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding).
Root Port	The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the spanning tree network.
Designated Root	The priority and MAC address of the device in the spanning tree that this switch has accepted as the root device.
Root Path Cost	The path cost from the root port on this switch to the root device.
Configuration Changes	The number of times the spanning tree has been reconfigured.
Last Topology Change	The time since the spanning tree was last reconfigured.

Ports

The parameters shown in the following figure and table are for port STA Information (Port 1-8).



Port	Port Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port
1	No Link	0	4	32768.00E06376F500	128.1
2	No Link	0	4	32768.00E06376F500	128.2
3	No Link	0	4	32768.00E06376F500	128.3
4	No Link	0	4	32768.00E06376F500	128.4
5	Forwarding	1	0	32768.000011114321	128.3
6	No Link	0	4	32768.00E06376F500	128.6
7	No Link	0	4	32768.00E06376F500	128.7
8	No Link	0	4	32768.00E06376F500	128.8

Figure 3-14. STA Information - Ports

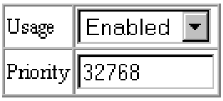
Parameter	Description
Port Status	Displays the current state of this port within the spanning tree: No Link There is no valid link on the port. Disabled Port has been disabled by the user or has failed diagnostics. Blocked Port receives STA configuration messages, but does not forward packets. Listening Port will leave blocking state due to topology change, starts transmitting configuration messages, but does not yet forward packets. Learning Has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses. Forwarding The port forwards packets, and continues learning addresses. The rules defining port status are: • A port on a network segment with no other STA-compliant bridging device is always forwarding. • If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is blocked. • All ports are blocked when the switch is booted, then some of them change state to listening, to learning, and then to forwarding.
Forward Transitions	The number of times the port has changed status to forwarding state.
Designated Cost	The cost for a packet to travel from this port to the root in the current spanning tree configuration. The slower the media, the higher the cost.

Parameter	Description
Designated Bridge	The priority and MAC address of the device through which this port must communicate to reach the root of the spanning tree.
Designated Port	The priority and number of the port on the designated bridging device through which this switch must communicate with the root of the spanning tree.

Spanning Tree Configuration

The following figures and tables describe Bridge STA configuration.

Switch

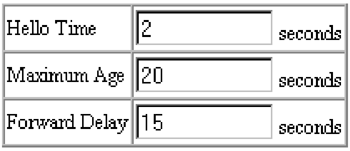


Usage	Enabled
Priority	32768

Figure 3-15. STA Configuration - Switch

Parameter	Default	Description
Usage	Enabled	Enable this parameter to participate in an STA-compliant network.
Priority	32,768	Device priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. (Remember that the lower the numeric value, the higher the priority.) However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Range: 0 - 65535

When the Switch Becomes Root



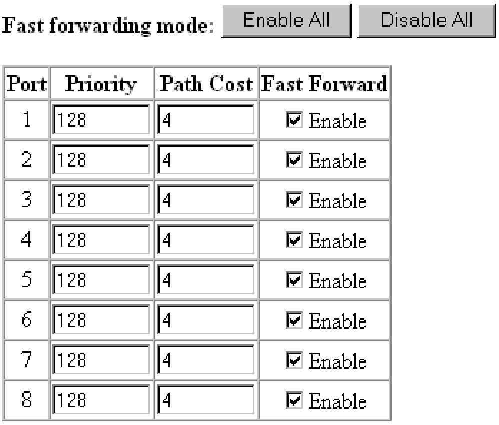
Hello Time	2	seconds
Maximum Age	20	seconds
Forward Delay	15	seconds

Figure 3-16. STA Configuration - When the Switch Becomes Root

Parameter	Default	Description
Hello Time	2	The time interval (in seconds) at which the root device transmits a configuration message. The minimum value is 1. The maximum value is the lower of 10 or [(Max. Message Age / 2) -1].
Max (Message) Age	20	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. The minimum value is the higher of 6 or [2 x (Hello Time + 1)]. The maximum value is the lower of 40 or [2 x (Forward Delay - 1)].
Forward Delay	15	The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. Maximum value is 30. Minimum value is the higher of 4 or [(Max. Message Age / 2) + 1].

STA Port Configuration

The following figure and table describe STA configuration for ports.



Fast forwarding mode:

Port	Priority	Path Cost	Fast Forward
1	128	4	☑ Enable
2	128	4	☑ Enable
3	128	4	☑ Enable
4	128	4	☑ Enable
5	128	4	☑ Enable
6	128	4	☑ Enable
7	128	4	☑ Enable
8	128	4	☑ Enable

Figure 3-17. STA Port Configuration

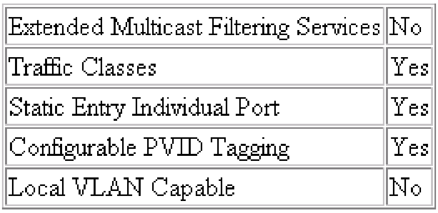
Parameter	Default	Description
Fast forwarding mode	ENABLED	Allows you to enable or disable fast forwarding for all ports on the switch.
Priority	128	Defines the priority for the use of a port in the STA algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the spanning tree. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. The range is 0 - 255.
(Path) Cost	100/19/4	This parameter is used by the STA algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. The default and recommended range is: Standard Ethernet: 100 (50-600) Fast Ethernet: 19 (10-60) Gigabit Ethernet: 4 (3-10) The full range is 1 - 65535. Note: Path cost takes precedence over port priority.

Parameter	Default	Description
FastForwarding	ENABLED	This parameter is used to enable/disabled the Fast Spanning Tree mode for the port. In this mode, ports skip the Blocked, Listening and Learning states and proceed straight to Forwarding. FastForwarding enables end-node workstations and servers to overcome time-out problems when the Spanning Tree Algorithm is implemented in a network. Therefore, FastForwarding should only be enabled for ports that are connected to an end-node device.

Configuring Bridge MIB Extensions

The Bridge MIB includes extensions for managed devices that support Traffic Classes, Multicast Filtering and Virtual LANs. To configure these extensions, use the Extended Bridge Configuration screen as shown below:

Bridge Capability

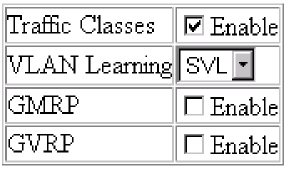


Extended Multicast Filtering Services	No
Traffic Classes	Yes
Static Entry Individual Port	Yes
Configurable PVID Tagging	Yes
Local VLAN Capable	No

Figure 3-18. Bridge Capability

Parameter	Description
Extended Multicast Filtering Services	Indicates that the switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol). Note that this function is not implemented in the current firmware release.
Traffic Classes	Indicates that the switch provides mapping of user priorities to multiple traffic classes. (Refer to the Priority menu on page 28.)
Static Entry Individual Port	Indicates that the switch allows the static filtering of unicast and multicast addresses. (Refer to the Address Table Configuration on page 19.)
Configurable PVID Tagging	Indicates that the switch allows you to override the default PVID setting (Port VLAN ID used in frame tags) and its egress status (VLAN-Tagged or Untagged) on each port. (Refer to VLAN Port Configuration on page 36.)
Local VLAN Capable	This switch does not support multiple local bridges (that is, multiple Spanning Trees).

Bridge Settings



Traffic Classes	☑ Enable
VLAN Learning	SVL ▾
GMRP	□ Enable
GVRP	□ Enable

Figure 3-19. Bridge Settings

Parameter	**Description**
Traffic Class*	Multiple traffic classes are supported by this switch as indicated under Bridge Capabilities. However, you can disable this function by clearing this checkbox.
VLAN Learning	As default this switch uses Shared VLAN Learning (SVL), whereby all ports share one VLAN filtering database. However, you can set the switch to use Independent VLAN Learning (IVL), where each port maintains its own filtering database. Note that when you change from one method to the other, the switch will automatically reset and the current VLAN configuration will be lost.
GMRP*	GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. Note that this function is not implemented in the current firmware release. The Internet Group Management Protocol (IGMP) is currently used by this switch to provide automatic multicast filtering.
GVRP*	GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports across the network. This function should be enabled to permit VLANs groups which extend beyond the local switch.

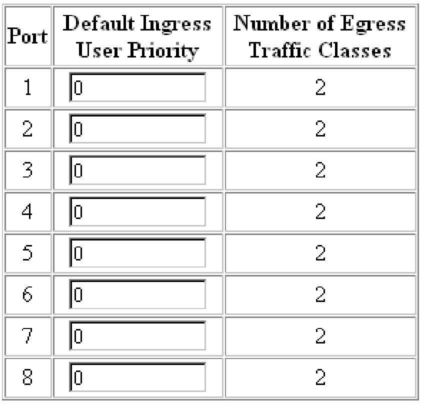
*** Not implemented in the current firmware release.**

Priority

IEEE 802.1p defines up to 8 separate traffic classes. This switch supports Quality of Service (QoS) by using two priority queues, with weighted fair queuing for each port. You can use the Priority menu to configure the default priority for each port, or to display the mapping for the traffic classes as described in the following sections.

Port Priority Configuration

The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in the low priority output queue. Default priority is only used to determine the output queue for the current port; no priority tag is actually added to the frame. You can use the Port Priority Configuration screen to adjust default priority for any port as shown below:



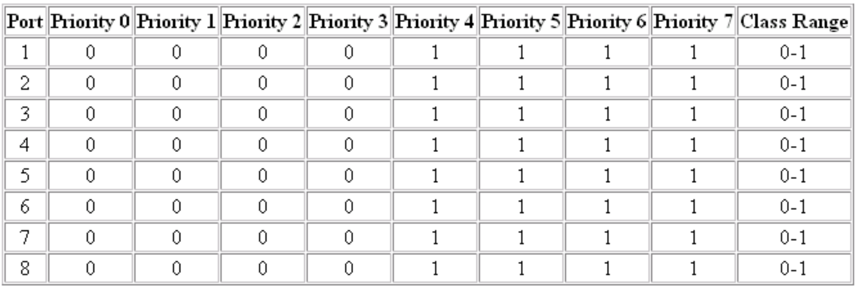
Port	Default Ingress User Priority	Number of Egress Traffic Classes
1	0	2
2	0	2
3	0	2
4	0	2
5	0	2
6	0	2
7	0	2
8	0	2

Figure 3-20. Port Priority Configuration

Parameter	Description
Port	Numeric identifier for switch port.
Default Ingress User Priority	Default priority can be set to any value from 0-7, where 0-3 specifies the low priority queue and 4-7 specifies the high priority queue.
Number of Egress Traffic Classes	Indicates that this switch supports two priority output queues.

Port Traffic Class Information

This switch provides two priority levels with weighted fair queuing for port egress. This means that any frames with a default or user priority from 0-3 are sent to the low priority queue “0” while those from 4-7 are sent to the high priority queue “1” as shown in the following screen:



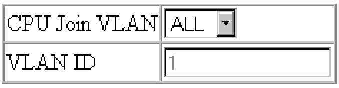
Port	Priority 0	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5	Priority 6	Priority 7	Class Range
1	0	0	0	0	1	1	1	1	0-1
2	0	0	0	0	1	1	1	1	0-1
3	0	0	0	0	1	1	1	1	0-1
4	0	0	0	0	1	1	1	1	0-1
5	0	0	0	0	1	1	1	1	0-1
6	0	0	0	0	1	1	1	1	0-1
7	0	0	0	0	1	1	1	1	0-1
8	0	0	0	0	1	1	1	1	0-1

Figure 3-21. Port Traffic Class Information

Parameter	Description
Port	Numeric identifier for switch port.
User Priority	Shows that user priorities 0-3 specify the low priority queue and 4-7 specify the high priority queue.

VLAN Management

Use the VLAN Management screen to define which VLAN has management access to the switch. Parameters shown on this screen are indicated in the following figure and table.:



CPU Join VLAN	ALL
VLAN ID	1

Figure 3-22. VLAN Management

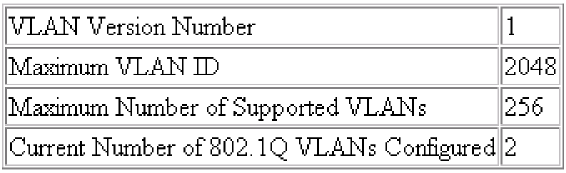
Parameter	Default	Description
CPU Join VLAN	All	Select ALL to give all VLANs access to switch management, or ONE to restrict access to a specified VLAN. If you select just one VLAN, you must specify its VLAN ID on the following line.
VLAN ID	1	Specifies the VLAN ID that has access to switch management.

Configuring Virtual LANs

You can use the VLAN configuration menu to assign any port on the switch to any of up to 256 LAN groups. In conventional networks with routers, broadcast traffic is split up into separate domains. Switches do not inherently support broadcast domains. This can lead to broadcast storms in large networks that handle a lot of IPX and NetBeui traffic. By using IEEE 802.1Q compliant VLANs and GARP VLAN Registration Protocol, you can organize any group of network nodes into separate broadcast domains, confining broadcast traffic to the originating group. This also provides a more secure and cleaner network environment. For more information on how to use VLANs, refer to “Virtual LANs” in the DNswitch 800 Management Guide. The VLAN configuration screens are described in the following sections.

VLAN Basic Information

The VLAN Basic Information screen displays basic information on the VLAN type supported by this switch.



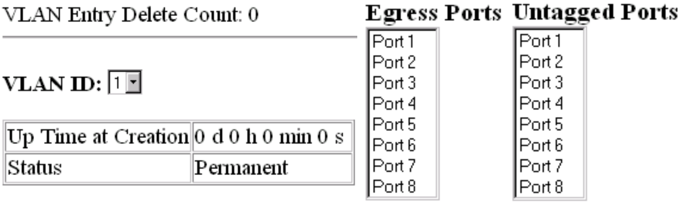
VLAN Version Number	1
Maximum VLAN ID	2048
Maximum Number of Supported VLANs	256
Current Number of 802.1Q VLANs Configured	2

Figure 3-23. VLAN Basic Information

Parameter	**Description**
VLAN Version Number	The VLAN version used by this switch as specified in the IEEE 802.1Q standard.
MAX VLAN ID	Maximum VLAN ID recognized by this switch.
MAX Supported VLANs	Maximum number of VLANs that can be configured on this switch.
Current Number of VLANs Configured	The number of VLANs currently configured on this switch.

VLAN Current Table

This screen shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can assign ports to the same untagged VLAN (page 36). The current configuration is shown in the following screen.



VLAN Entry Delete Count: 0

VLAN ID: 1

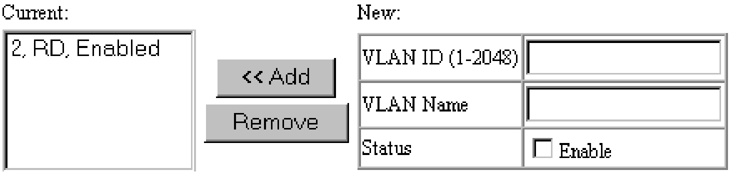
Up Time at Creation	0 d 0 h 0 min 0 s
Status	Permanent

Figure 3-24. VLAN Current Table

Parameter	Description
VLAN Entry Delete Count	The number of times a VLAN entry has been deleted from this table.
VLAN ID	The ID for the VLAN currently displayed.
Up Time at Creation	The value of sysUpTime (System Up Time) when this VLAN was created.
Status	Shows how this VLAN was added to the switch: Dynamic GVRP: Automatically learned via GVRP. Permanent: Added as a static entry.
Egress Ports	Shows the ports which have been added to the displayed VLAN group.
Untagged Ports	Shows the untagged VLAN port members.

VLAN Static List

Use this screen to create or remove VLAN groups.



Current:

2, RD, Enabled

New:

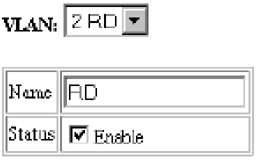
VLAN ID (1-2048)	
VLAN Name	
Status	□ Enable

Figure 3-25. VLAN Static List

Parameter	Description
Current	Lists all the current VLAN groups created for this system. Up to 256 VLAN groups can be defined. To allow this switch to participate in external VLAN groups, you must use the VLAN ID for the concerned external groups.
New	Allows you to specify the name and numeric identifier for a new VLAN group. (The VLAN name is only used for management on this system; it is not added to the VLAN tag.)
Status	Enables/disables the specified VLAN.
Add	Adds a new VLAN group to the current list.
Remove	Removes a VLAN group from the current list. If any port is assigned to this group as untagged, it will be reassigned to VLAN group 1 as untagged.

VLAN Static Table

Use this screen to modify the settings for an existing VLAN. You can add/delete port members for a VLAN, disable or enable VLAN tagging for any port, or prevent a port from being automatically added to a VLAN via the GVRP protocol. (Note that VLAN1 is fixed as an untagged VLAN containing all ports on the switch, and cannot be modified via this screen.)



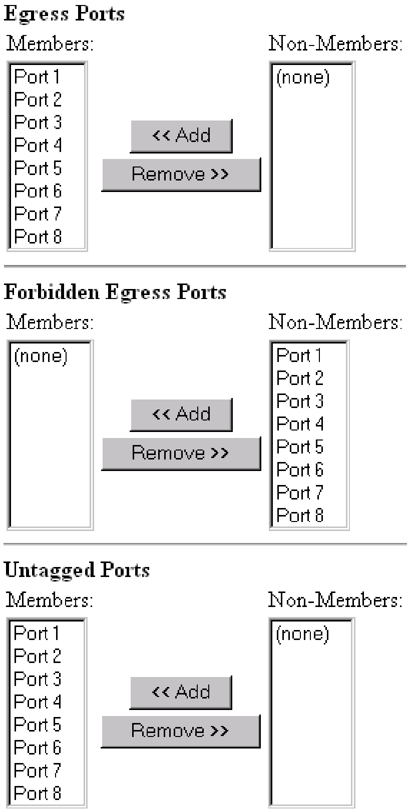
VLAN: 2 RD

Name	RD
Status	☑ Enable

Figure 3-26. VLAN Static Table - Add/Modify VLAN

Parameter	Description
VLAN	The ID for the VLAN currently displayed. Range: 1-2048
Name	A user-specified symbolic name for this VLAN. String length: 8 alphanumeric characters
Status	Enables/disables the specified VLAN.

Use the screens shown below to assign ports to the specified VLAN group as an IEEE 802.1Q tagged port. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices. If the port is connected to VLAN-unaware devices, frames will passed to the untagged VLAN group this port has been assigned to under VLAN Port Configuration (page 36).



Egress Ports

Members: Port 1, Port 2, Port 3, Port 4, Port 5, Port 6, Port 7, Port 8

Non-Members: (none)

Forbidden Egress Ports

Members: (none)

Non-Members: Port 1, Port 2, Port 3, Port 4, Port 5, Port 6, Port 7, Port 8

Untagged Ports

Members: Port 1, Port 2, Port 3, Port 4, Port 5, Port 6, Port 7, Port 8

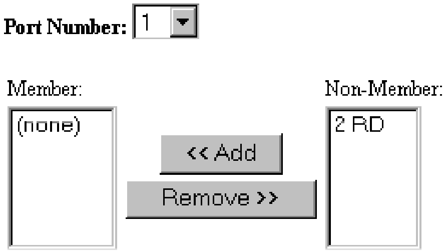
Non-Members: (none)

Figure 3-27. VLAN Static Table - Port Assignment

Parameter	Description
Egress Ports	Adds ports to the specified VLAN.
Forbidden Egress Ports	Prevents a port from being automatically added to this VLAN via GVRP.
Untagged Ports	Adds untagged ports to the specified VLAN.

VLAN Static Membership by Port

Use the screen shown below to assign VLAN groups to the selected port. To perform detailed port configuration for a specific VLAN, use the VLAN Static Table (page 33).



Port Number: 1

Member: (none)

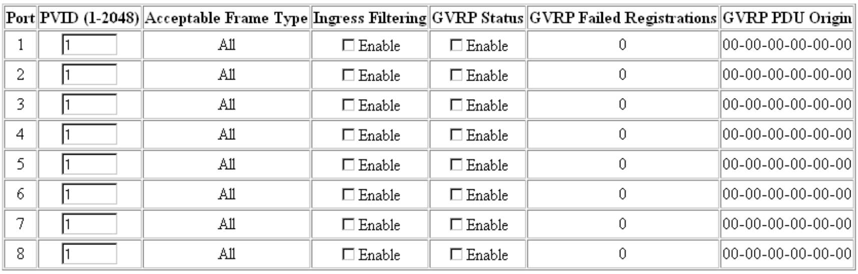
Non-Member: 2 RD

Figure 3-28. VLAN Static Membership by Port

Parameter	Description
Port Number	Port number on the switch selected from the upper display panel.
Add/Remove	Add or remove selected VLAN groups for the port indicated in the Port Number field.

VLAN Port Configuration

Use this screen to configure port-specific settings for IEEE 802.1Q VLAN features.



Port	PVID (1-2048)	Acceptable Frame Type	Ingress Filtering	GVRP Status	GVRP Failed Registrations	GVRP PDU Origin
1	1	All	□ Enable	□ Enable	0	00-00-00-00-00-00
2	1	All	□ Enable	□ Enable	0	00-00-00-00-00-00
3	1	All	□ Enable	□ Enable	0	00-00-00-00-00-00
4	1	All	□ Enable	□ Enable	0	00-00-00-00-00-00
5	1	All	□ Enable	□ Enable	0	00-00-00-00-00-00
6	1	All	□ Enable	□ Enable	0	00-00-00-00-00-00
7	1	All	□ Enable	□ Enable	0	00-00-00-00-00-00
8	1	All	□ Enable	□ Enable	0	00-00-00-00-00-00

Figure 3-29. VLAN Port Configuration

Parameter	Description
PVID	The VLAN ID assigned to untagged frames received on this port. Use the PVID to assign ports to the same untagged VLAN.
Acceptable Frame Type[1]	This switch accepts "All" frame types, including VLAN tagged or VLAN untagged frames. Note that all VLAN untagged frames received on this port are assigned to the PVID for this port.
Ingress Filtering[1]	If set to "True," incoming frames for VLANs which do not include this port in their member set will be discarded at the inbound port.
GVRP Status[2]	Enables or disables GVRP for this port. When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. Note that GVRP must be enabled for the switch before this port setting can take effect. (See Configuring Bridge MIB Extensions on page 26.)
GVRP Failed Registrations[2]	The total number of failed GVRP registrations, for any reason, on this port.
GVRP Last PDU Origin[2]	The Source MAC Address of the last GVRP message received on this port.

[1] **This control does not affect VLAN independent BPDU frames, such as GVRP or STP. However, it does affect VLAN dependent BPDU frames, such as GMRP.**

[2] **Note that GVRP is not implemented in the current firmware release.**

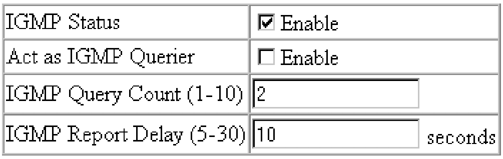
IGMP Multicast Filtering

Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts which want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on the hosts which subscribed to this service.

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts who want to receive a specific multicast service. The switch looks up the IP Multicast Group used for this service and adds any port which received a similar request to that group. It then propagates the service request on to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service. (For more information, see “IP Multicast Filtering” in the DNswitch 800 Management Guide.)

Configuring IGMP

This protocol allows a host to inform its local switch/router that it wants to receive transmissions addressed to a specific multicast address group. Use the IGMP Configuration screen to set key parameters for multicast filtering as shown below.



IGMP Status	☑ Enable
Act as IGMP Querier	☐ Enable
IGMP Query Count (1-10)	2
IGMP Report Delay (5-30)	10 seconds

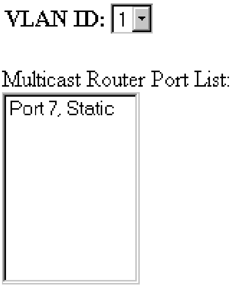
Figure 3-30. IGMP Configuration

Parameter	Description
IGMP Status	If enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic.
Act as IGMP Querier	If enabled, the switch can serve as the “querier,” which is responsible for asking hosts if they want to receive multicast traffic. (Not available for the current firmware release.)
IGMP Query Count	The maximum number of queries issued for which there has been no response before the switch takes action to solicit reports. (Range: 2 - 10.)
IGMP Report Delay	The time (in seconds) between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out that port and removes the entry from its list. (Range: 5 - 30.)

Note: The default values are indicated in the sample screen.

Multicast Router Port Information

You can use the Multicast Router Port Information screen to display the ports on this switch that are attached to a neighboring multicast router/ switch for each VLAN ID.



VLAN ID: 1

Multicast Router Port List:

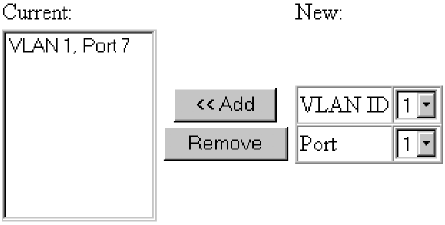
Port 7, Static

Figure 3-31. Multicast Router Port Information

Parameter	Description
VLAN ID	The VLAN ID assigned to the multicast group in the displayed port list.
Multicast Router Port List	The list of switch ports that are attached to a neighboring multicast router/switch.

Static Multicast Router Port Configuration

You can use the Static Multicast Router Port Configuration screen to assign ports that are attached to a neighboring multicast router/switch.



Current:

VLAN 1, Port 7

New:

VLAN ID 1

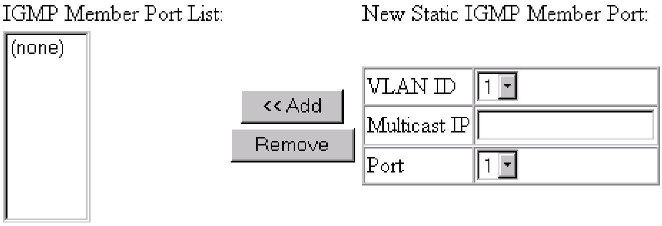
Port 1

Figure 3-32. Static Multicast Router Port Configuration

Parameter	Description
Current	A list of the switch ports that have been manually configured as being attached to a neighboring multicast router/switch.
VLAN ID	The VLAN ID assigned to the multicast group that is to be added/ removed from the list.
Port	The port number of a port to be added/removed from the list.
Add	Adds a new router port to the current list.
Remove	Removes a router port from the current list.

IGMP Member Port Table

You can use the IGMP Member Port Table screen to assign ports that are attached to hosts who want to receive a specific multicast service.



IGMP Member Port List:

(none)

New Static IGMP Member Port:

VLAN ID: 1

Multicast IP:

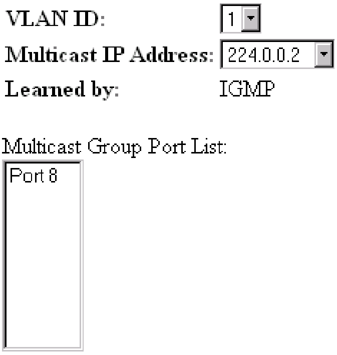
Port: 1

Figure 3-33. IGMP Member Port Table

Parameter	Description
IGMP Member Port List	The current switch ports that are listed as being attached to a IGMP host.
VLAN ID	The VLAN ID assigned to this multicast group.
Multicast IP	The IP address of a specific multicast service requested by the host.
Port	The port number of a port to be added/removed from the list.
Add	Adds a new host port to the current list.
Remove	Removes a host port from the current list.

IP Multicast Registration Table

Use the IP Multicast Registration Table to display all the multicast groups active on this switch, including multicast IP addresses and the corresponding VLAN ID.



VLAN ID: 1

Multicast IP Address: 224.0.0.2

Learned by: IGMP

Multicast Group Port List:

Port 8

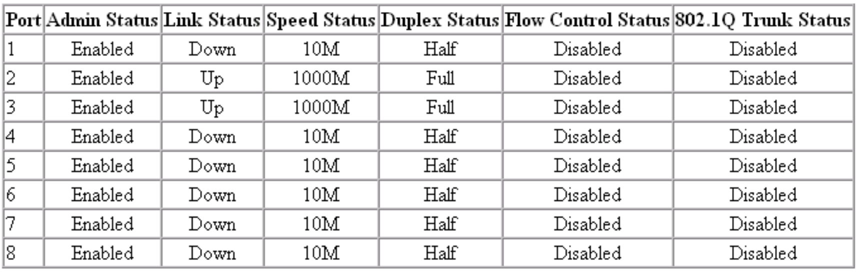
Figure 3-34. IP Multicast Registration Table

Parameter	Description
VLAN ID	VLAN ID assigned to this multicast group.
Multicast IP Address	IP address for specific multicast services.
Learned by	Indicates the manner in which this address was learned: dynamic or IGMP.
Multicast Group Port List	The switch ports registered for the indicated multicast service.

Port Menus

Port Information

The Port Information screen displays the port status, link state, the communication speed and duplex mode, as well as the flow control and 802.1Q Trunk status. To change any of the port settings, use the Port Configuration menu. The parameters shown in the following figure and table are for the RJ-45 ports.



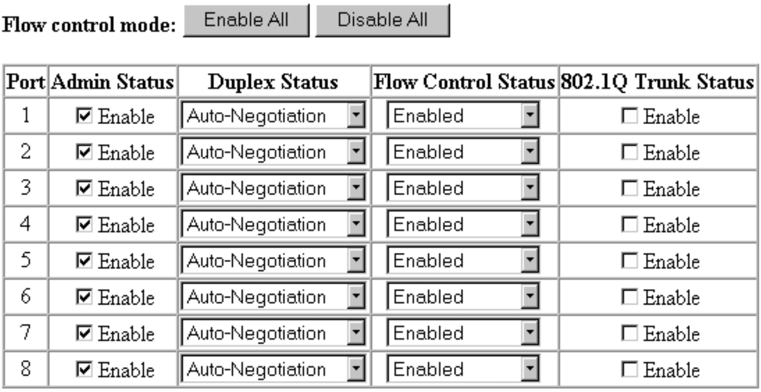
Port	Admin Status	Link Status	Speed Status	Duplex Status	Flow Control Status	802.1Q Trunk Status
1	Enabled	Down	10M	Half	Disabled	Disabled
2	Enabled	Up	1000M	Full	Disabled	Disabled
3	Enabled	Up	1000M	Full	Disabled	Disabled
4	Enabled	Down	10M	Half	Disabled	Disabled
5	Enabled	Down	10M	Half	Disabled	Disabled
6	Enabled	Down	10M	Half	Disabled	Disabled
7	Enabled	Down	10M	Half	Disabled	Disabled
8	Enabled	Down	10M	Half	Disabled	Disabled

Figure 3-35. Port Information

Parameter	Description
Admin Status	Shows if the port is enabled or not.
Link Status	Indicates if the port has a valid connection to an external device.
Speed Status	Shows the port speed (1000M).
Duplex Status	Displays the current duplex mode.
Flow Control Status	Shows the flow control type in use. Flow control can eliminate frame loss by “blocking” traffic from end stations connected directly to the switch. Back pressure is used for half duplex and IEEE 802.3x for full duplex.
802.1Q Trunk Status	Shows the VLAN trunk status for the port. A VLAN Trunk link between two VLAN-aware switches will carry traffic from all VLANs, allowing VLAN tagged frames to maintain their VLAN ID across multiple switches. When enabled, a port joins all configured VLANs and the untagged port VLAN ID (PVID) is set to 4000, a reserved VLAN ID for trunk ports.

Port Configuration

Use the Port Configuration menus to configure any port on the switch.



Flow control mode: [Enable All] [Disable All]

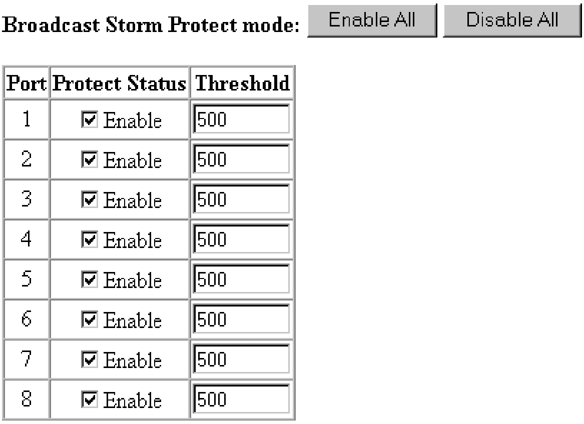
Port	Admin Status	Duplex Status	Flow Control Status	802.1Q Trunk Status
1	☑ Enable	Auto-Negotiation	Enabled	□ Enable
2	☑ Enable	Auto-Negotiation	Enabled	□ Enable
3	☑ Enable	Auto-Negotiation	Enabled	□ Enable
4	☑ Enable	Auto-Negotiation	Enabled	□ Enable
5	☑ Enable	Auto-Negotiation	Enabled	□ Enable
6	☑ Enable	Auto-Negotiation	Enabled	□ Enable
7	☑ Enable	Auto-Negotiation	Enabled	□ Enable
8	☑ Enable	Auto-Negotiation	Enabled	□ Enable

Figure 3-36. Port Configuration

Parameter	Default	Description
Flow Control Mode	Enabled	Allows you to enable or disable flow control for all ports on the switch.
Admin Status	Enable	Allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable a port for security reasons.
Duplex Status	Auto-Negotiation	Used to set the current port duplex mode or auto-negotiation. The default is auto-negotiation.
Flow Control status	Enabled	Used to enable or disable flow control. Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. Back pressure is used for half duplex and IEEE 802.3x for full duplex. Note that flow control should not be used if a port is connected to a hub.
802.1Q Trunk Status	Disabled	Used to enable/disable the VLAN trunk status for the port. A VLAN Trunk link between two VLAN-aware switches will carry traffic from all VLANs, allowing VLAN tagged frames to maintain their VLAN ID across multiple switches. When enabled, a port joins all configured VLANs and the untagged port VLAN ID (PVID) is set to 4000, a reserved VLAN ID for trunk ports.

Port Broadcast Storm Protect Configuration

Use the Port Broadcast Storm Protect Configuration screen to configure broadcast storm control for any port on the switch.



Broadcast Storm Protect mode: Enable All Disable All

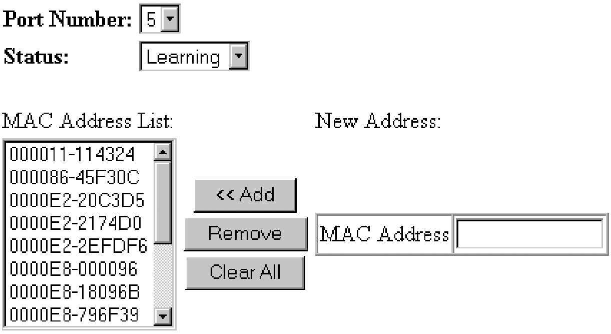
Port	Protect Status	Threshold
1	☑ Enable	500
2	☑ Enable	500
3	☑ Enable	500
4	☑ Enable	500
5	☑ Enable	500
6	☑ Enable	500
7	☑ Enable	500
8	☑ Enable	500

Figure 3-37. Port Broadcast Storm Protect Configuration

Parameter	Default	Description
Broadcast Storm Protect Mode	Enabled	Allows you to enable/disable broadcast storm control for all ports on the switch.
Protect Status	Enabled	Enables/disables broadcast control for the port. When enabled, the switch will employ a broadcast-control mechanism if the packet-per-second threshold is exceeded. This mechanism limits the amount of broadcasts passed by the port to half of the received packet-per-second count. The control mechanism remains in effect until the number of received broadcasts falls back below the packet-per-second threshold.
Threshold	500	The packet-per-second threshold at which broadcast control will be employed on the port.

Port Security Configuration

Use the Port Security Configuration screen to enable and configure port security for the switch. Port Security allows you to configure each port with a list of MAC addresses of devices that are authorized to access the network through that port.



Port Number: 5

Status: Learning

MAC Address List:

000011-114324
000086-45F30C
0000E2-20C3D5
0000E2-2174D0
0000E2-2EFDF6
0000E8-000096
0000E8-18096B
0000E8-796F39

New Address:

MAC Address

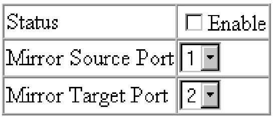
Figure 3-38. Port Security Configuration

Parameter	Description
Port Number	The port number on the unit.
Status	Port security can set to three states; Enabled, Disabled, or Learning. When set to Enabled, the switch will drop packets from the port if the source MAC address does not match one of the addresses in the MAC Address list. If set to Learning, the switch will use the last valid source address to filter packets from the port.
MAC Address List	A list of the current authorized MAC addresses that can access the network through the specified port.
MAC Address	A specific MAC address to be added or deleted from the list. A MAC address must be entered as 12 hexadecimal digits in the format “000000-000000” or “000000000000” to be correctly accepted by the system.
Add	Adds a new MAC address to the current list.
Remove	Removes a MAC address from the current list.
Clear All	Clears all the MAC addresses for the current port.

Using a Port Mirror for Analysis

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner. When mirroring port traffic, note that the target port must be configured in the same VLAN and be operating at the same duplex mode as the source port (see VLAN Static List on page 33).

You can use the port mirror configuration screen to designate a single port pair for mirroring as shown below:



Status	□ Enable
Mirror Source Port	1 ▾
Mirror Target Port	2 ▾

Figure 3-39. Mirror Port Configuration

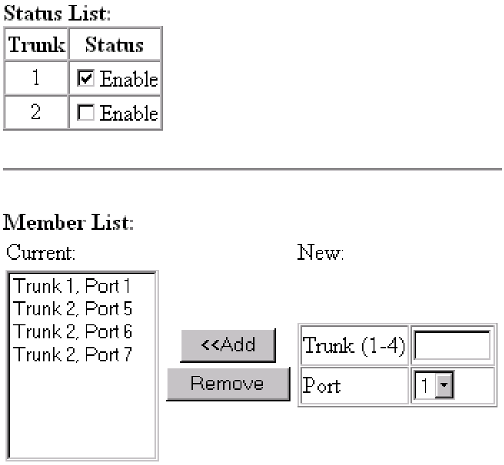
Parameter	Description
Status	Enables/disables port mirroring.
Mirror Source Port	The port whose traffic will be monitored.
Mirror Target Port	The port that will duplicate or “mirror” all the traffic happening on the monitored port.

Port Trunk Configuration

Port trunks can be used to increase the bandwidth of a network connection or to ensure fault recovery. You can configure up four trunk connections (combining 2-4 ports into a fat pipe) between any two DNswitch 800 switches. However, before making any physical connections between devices, use the Trunk Configuration menu to specify the trunk on the devices at both ends. When using a port trunk, note that:

- Ports can only be assigned to one trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- The ports at both ends of a trunk must be configured in an identical manner, including duplex mode and VLAN assignments.
- None of the ports in a trunk can be configured as a mirror source port or mirror target port.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- The Spanning Tree Algorithm will treat all the ports in a trunk as a whole.
- Enable the trunk prior to connecting any cable between the switches to avoid creating a loop.
- Disconnect all trunk port cables or disable the trunk ports before removing a port trunk to avoid creating a loop.

Use the Port Trunking Configuration screen to set up port trunks as shown below:



Status List:

Trunk	Status
1	☑ Enable
2	☐ Enable

Member List:

Current:

Trunk 1, Port 1
Trunk 2, Port 5
Trunk 2, Port 6
Trunk 2, Port 7

New:

Trunk (1-4)	
Port	1

Figure 3-40. Port Trunk Configuration

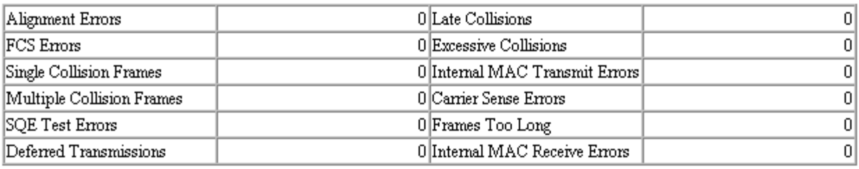
Parameter	Description
Trunk Number	A unique identifier for this trunk. You can configure up to four trunks per switch.
Port	The port members of this trunk. Select from 2-4 ports per trunk.

Port Statistics

Use the Port Statistics menu to display Etherlike or RMON statistics for any port on the switch. Select the required port. The statistics displayed are indicated in the following figure and table.

Etherlike Statistics

Etherlike Statistics display key statistics from the Ethernet-like MIB for each port. Error statistics on the traffic passing through each port are displayed. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). Values displayed have been accumulated since the last system reboot.



Alignment Errors	0	Late Collisions	0
FCS Errors	0	Excessive Collisions	0
Single Collision Frames	0	Internal MAC Transmit Errors	0
Multiple Collision Frames	0	Carrier Sense Errors	0
SQE Test Errors	0	Frames Too Long	0
Deferred Transmissions	0	Internal MAC Receive Errors	0

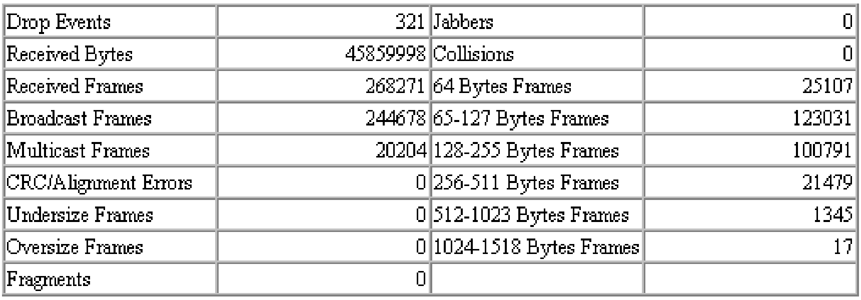
Figure 3-41. Etherlike Statistics

Parameter	Description
Alignment Errors	The number of frames received that are not an integral number of octets in length and do not pass the FCS check.
FCS Errors	The number of frames received that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames*	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames*	A count of successfully transmitted frames for which transmission is inhibited by more that one collision.
SQE Test Errors*	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer.
Deferred Transmissions*	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collisions*	The number of frames for which transmission failed due to excessive collisions.
Internal Mac Transmit Errors*	The number of frames for which transmission failed due to an internal MAC sublayer transmit error.
Carrier Sense Errors*	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Frames Too Long	The number of frames received that exceed the maximum permitted frame size.
Internal Mac Receive Errors*	The number of frames for which reception failed due to an internal MAC sublayer receive error.

*** The reported values will always be zero because these statistics are not supported by the internal chip set.**

RMON Statistics

RMON Statistics display key statistics for each port from RMON group 1. (RMON groups 2, 3 and 9 can only be accessed using SNMP management software.) The following screen displays overall statistics on traffic passing through each port. RMON statistics provide access to a broad range of statistics, including a total count of different frame types passing through each port. Values displayed have been accumulated since the last system reboot.



Drop Events	321	Jabbers	0
Received Bytes	45859998	Collisions	0
Received Frames	268271	64 Bytes Frames	25107
Broadcast Frames	244678	65-127 Bytes Frames	123031
Multicast Frames	20204	128-255 Bytes Frames	100791
CRC/Alignment Errors	0	256-511 Bytes Frames	21479
Undersize Frames	0	512-1023 Bytes Frames	1345
Oversize Frames	0	1024-1518 Bytes Frames	17
Fragments	0		

Figure 3-42. RMON Statistics

Parameter	Description
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC/Alignment Errors	The number of frames received with CRC/alignment errors (FCS or alignment errors).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.

Parameter	Description
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Byte Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames	The total number of frames (including bad packets) received and transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256-511 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

APPENDIX A. TROUBLESHOOTING

This appendix describes problems potentially encountered when using Digital Networks WebView and presents suggested solutions for correcting these problems.

Troubleshooting

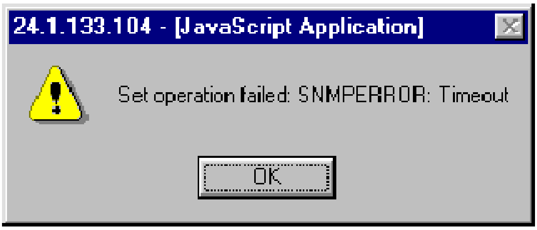
Cannot Connect to the Switch

If you attempt to connect to the switch and the main window does not appear, make sure that the correct IP address is entered in the URL field of the browser.

- Check the network connections of both your workstation and the switch.
- Try to Ping the IP address to see If it's indeed reachable.
- Set the IP gateway if necessary.
- Make sure the correct password is entered.
- Make sure the HTTP Server parameter is set to "ENABLED."

System is Disconnected from the Switch

If your workstation is disconnected from the switch during an active session, you may see the following messages:



24.1.133.104 - [JavaScript Application]

Set operation failed: SNMPERROR: Timeout

or, "Device is not responding to SNMP queries"

- Reconnect the workstation to the switch. You may need to re-enter your latest changes, but the user interface should become available again for use.
- If the user interface does not become available after reconnecting, close the Digital Networks WebView window and start a new session.

Frequently Asked Questions

Can I Open More Than One Window for Same Switch?

Yes. You can start multiple browser sessions with the switch at once.

Will Network Congestion Prevent Use of Digital Networks WebView?

It could. If there is significant network delay after a configuration command is issued, the system could time out. In addition, excessive delays when gathering switch statistics could interfere with the accuracy of performance statistics.

How Do I Confirm a Successful Software Download?

After the download is complete, go to the Switch Information screen to verify that the software version running on the switch is the same as the software just upgraded. If the version has not been upgraded, retry the procedure.

INDEX

Digital Networks

digital™